

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-069598

(43)Date of publication of application : 07.03.2003

(51)Int.Cl.

H04L 12/46

(21)Application number : 2001-253225

(71)Applicant : ALLIED TERESHISU KK

(22)Date of filing : 23.08.2001

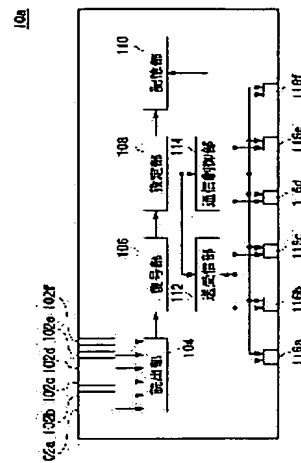
(72)Inventor : SATO TAKAYUKI
HANEDA JUN

(54) RELAY APPARATUS, COMMUNICATION SETTING PROGRAM, AND COMMUNICATION SETTING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a relay apparatus realizing a computer network system which is very high in security against unauthorized access.

SOLUTION: The relay apparatus, which relays communication in a computer network, is provided with the first holding portion for holding a removable nonvolatile memory, a reading portion for reading, from the nonvolatile memory held in a first holding portion, a first apparatus identifying information of a first communication apparatus to which the communication in the computer network is permitted, and a setting portion for performing a communication setting of the computer network in order to permit the communication in the computer network of the first communication apparatus identified by the first apparatus identifying information.



LEGAL STATUS

[Date of request for examination]

29.10.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the
examiner's decision of rejection or application
converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of
rejection][Date of requesting appeal against examiner's decision
of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-69598

(P 2 0 0 3 - 6 9 5 9 8 A)

(43) 公開日 平成15年3月7日(2003.3.7)

(51) Int. Cl. ⁷	識別記号	F I		テ-マコード (参考)
H04L 12/46	100	H04L 12/46	100	B 5K033

審査請求 未請求 請求項の数18 O L (全10頁)

(21) 出願番号	特願2001-253225 (P 2001-253225)	(71) 出願人	396008347 アライドテレシス株式会社 東京都品川区西五反田7-22-17 T O C ビル
(22) 出願日	平成13年8月23日(2001.8.23)	(72) 発明者	佐藤 貴之 東京都品川区西五反田7-22-17 T O C ビル アライドテレシス株式会社内
		(72) 発明者	羽田 純 東京都品川区西五反田7-22-17 T O C ビル アライドテレシス株式会社内
		(74) 代理人	100104156 弁理士 龍華 明裕 F ターム(参考) 5K033 AA08 BA04 CB08 CC01 DA05 DB10 DB18

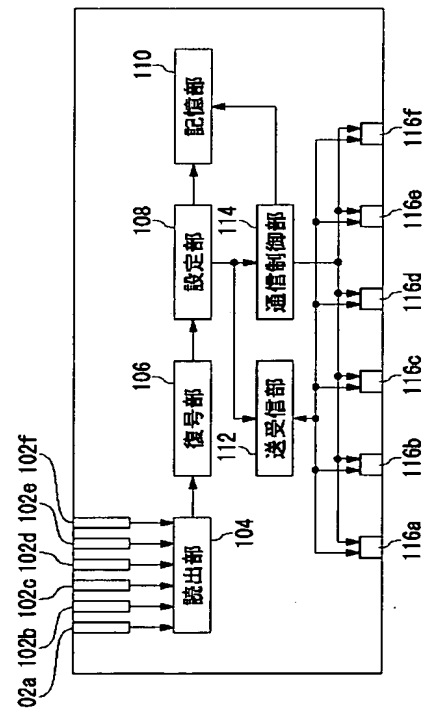
(54) 【発明の名称】 中継機器、通信設定プログラム、及び通信設定方法

(57) 【要約】

【課題】 不正進入に対するセキュリティが非常に高いコンピュータネットワークシステムを実現できる中継機器を提供する。

【解決手段】 コンピュータネットワークにおいて通信を中継する中継機器であって、着脱可能な不揮発性メモリを保持する第1保持部と、第1保持部に保持された不揮発性メモリから、コンピュータネットワークにおける通信が許可される第1通信機器の第1機器識別情報を読み出す読出部と、第1機器識別情報で識別される第1通信機器のコンピュータネットワークにおける通信を許可すべくコンピュータネットワークの通信設定を行う設定部とを備える。

10a



【特許請求の範囲】

【請求項 1】 コンピュータネットワークにおいて通信を中継する中継機器であって、

着脱可能な不揮発性メモリを保持する第 1 保持部と、
前記第 1 保持部に保持された前記不揮発性メモリから、
前記コンピュータネットワークにおける通信が許可される第 1 通信機器の第 1 機器識別情報を読み出す読出部と、

前記第 1 機器識別情報で識別される前記第 1 通信機器の前記コンピュータネットワークにおける通信を許可すべく前記コンピュータネットワークの通信設定を行う設定部とを備えることを特徴とする中継機器。

【請求項 2】 前記不揮発性メモリは、暗号化された前記第 1 機器識別情報を格納し、
前記読出部に読み出された前記第 1 機器識別情報を復号する復号部をさらに備えることを特徴とする請求項 1 に記載の中継機器。

【請求項 3】 前記設定部は、前記第 1 機器識別情報で識別される前記第 1 通信機器の当該中継機器における通信を許可すべく当該中継機器を設定することを特徴とする請求項 1 に記載の中継機器。

【請求項 4】 前記設定部は、前記第 1 機器識別情報で識別される前記第 1 通信機器による通信の、当該中継機器における帯域幅をさらに設定することを特徴とする請求項 3 に記載の中継機器。

【請求項 5】 前記第 1 機器識別情報で識別される前記第 1 通信機器の当該中継機器に接続された他の中継機器における通信を許可させるように設定させるべく、前記第 1 機器識別情報を前記他の中継機器に送信する送信部をさらに備えることを特徴とする請求項 3 に記載の中継機器。

【請求項 6】 前記他の中継機器は、前記コンピュータネットワークと、前記コンピュータネットワークの他のコンピュータネットワークとを接続しており、
前記送信部は、前記第 1 機器識別情報で識別される前記第 1 通信機器の前記他のコンピュータネットワークにおける通信を許可させるように設定させるべく、前記第 1 機器識別情報を前記他の中継機器に送信することを特徴とする請求項 5 に記載の中継機器。

【請求項 7】 前記第 1 機器識別情報で識別される前記第 1 通信機器の前記コンピュータネットワークにおける通信を許可するように設定させるべく、前記コンピュータネットワークを管理する管理装置に、前記第 1 機器識別情報を送信する送信部をさらに備えることを特徴とする請求項 3 に記載の中継機器。

【請求項 8】 着脱可能な不揮発性メモリを保持する第 2 保持部をさらに有し、
前記読出部は、前記第 2 保持部に保持された前記不揮発性メモリから、前記コンピュータネットワークにおける通信が許可される第 2 通信機器の第 2 機器識別情報を読

み出し、

前記設定部は、前記第 2 機器識別情報で識別される前記第 2 通信機器の前記コンピュータネットワークにおける通信を許可すべく前記コンピュータネットワークの前記通信設定を行うことを特徴とする請求項 1 に記載の中継機器。

【請求項 9】 前記設定部は、前記第 1 機器識別情報で識別される前記第 1 通信機器の当該中継機器における前記通信を許可すべく当該中継機器を設定し、前記第 2 機器識別情報で識別される前記第 2 通信機器の当該中継機器における前記通信を許可すべく当該中継機器を設定することを特徴とする請求項 8 に記載の中継機器。

【請求項 10】 前記第 1 通信機器が接続される第 1 接続ポートと、
前記第 2 通信機器が接続される第 2 接続ポートとをさらに備え、

前記設定部は、前記第 1 通信機器の前記第 1 接続ポートにおける通信と、前記第 2 通信機器の前記第 2 接続ポートにおける通信とを許可すべく、当該中継機器を設定することを特徴とする請求項 9 に記載の中継機器。

【請求項 11】 前記設定部は、前記第 1 接続ポート及び前記第 2 接続ポートを介する通信の帯域幅をさらに設定することを特徴とする請求項 10 に記載の中継機器。

【請求項 12】 当該中継機器における通信を許可する少なくとも 1 つの通信機器の機器識別情報を格納する記憶部と、
前記記憶部に格納された前記機器識別情報に基づいて、当該中継機器における通信を許可する通信機器を制限する通信制御部とをさらに備えることを特徴とする請求項 11 に記載の中継機器。

【請求項 13】 前記設定部は、前記読出部により読み出された前記第 1 機器識別情報で識別される前記第 1 通信機器の当該中継機器における通信を許可すべく、前記読出部により読み出された前記第 1 機器識別情報を前記記憶部に格納することを特徴とする請求項 12 に記載の中継機器。

【請求項 14】 当該中継機器は、複数の通信機器がそれぞれ接続される複数の接続ポートを有し、
前記記憶部は、前記複数の接続ポートのそれぞれに対応づけて、前記複数の接続ポートのそれぞれにおける通信を許可する少なくとも 1 つの通信機器の機器識別情報を格納することを特徴とする請求項 12 に記載の中継機器。

【請求項 15】 コンピュータネットワークの通信設定を行う中継機器用の通信設定プログラムであって、前記中継機器に、
着脱可能な不揮発性メモリから、前記コンピュータネットワークにおける通信が許可される通信機器の機器識別情報を読み出させる読出モジュールと、
前記機器識別情報で識別される前記通信機器の前記コン

コンピュータネットワークにおける通信を許可すべく前記コンピュータネットワークの通信設定を行わせる設定モジュールとを備えることを特徴とする通信設定プログラム。

【請求項 16】 前記設定モジュールは、前記機器識別情報で識別される前記通信機器の当該中継機器における通信を許可させるべく当該中継機器を設定させることを特徴とする請求項 15 に記載の通信設定プログラム。

【請求項 17】 前記機器識別情報で識別される前記通信機器の当該中継機器に接続された他の中継機器における通信を許可させるように設定させるべく、前記機器識別情報を前記他の中継機器に送信させる送信モジュールをさらに備えることを特徴とする請求項 16 に記載の通信設定プログラム。

【請求項 18】 コンピュータネットワークにおいて通信を中継する中継機器による前記コンピュータネットワークの通信設定方法であって、
着脱可能な不揮発性メモリを保持する保持段階と、
保持された前記不揮発性メモリから、前記コンピュータネットワークにおける通信が許可される通信機器の機器識別情報を読み出す読出段階と、
前記機器識別情報で識別される前記通信機器の前記コンピュータネットワークにおける通信を許可すべく前記コンピュータネットワークの通信設定を行う設定段階とを備えることを特徴とする通信設定方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、中継機器、通信設定プログラム、及び通信設定方法に関する。特に本発明は、コンピュータネットワークの通信設定を行う中継機器に関する。

【0002】

【従来の技術】従来、コンピュータネットワークを統括的に管理する管理サーバによって、任意のコンピュータによるコンピュータネットワークへの不正進入に対するセキュリティが実現されている。例えば、管理サーバによるユーザ認証、VLAN の設定等によってコンピュータネットワークへの進入の制限を行っている。

【0003】

【発明が解決しようとする課題】しかしながら、従来のコンピュータネットワークシステムでは、管理サーバによってコンピュータネットワークへの進入を制限しているため、ユーザが使用する任意のコンピュータは、コンピュータネットワークを介して管理サーバに接続する。そのため、実質的に任意のコンピュータによるコンピュータネットワークへの進入を制限する手段はなく、任意のコンピュータが容易にコンピュータネットワークにおいて通信を行うことができるという問題がある。

【0004】そこで本発明は、上記の課題を解決することのできる中継機器、通信設定プログラム、及び通信設

定方法を提供することを目的とする。この目的は特許請求の範囲における独立項に記載の特徴の組み合わせにより達成される。また従属項は本発明の更なる有利な具体例を規定する。

【0005】

【課題を解決するための手段】即ち、本発明の第 1 の形態によると、コンピュータネットワークにおいて通信を中継する中継機器であって、着脱可能な不揮発性メモリを保持する第 1 保持部と、第 1 保持部に保持された不揮発性メモリから、コンピュータネットワークにおける通信が許可される第 1 通信機器の第 1 機器識別情報を読み出す読出部と、第 1 機器識別情報で識別される第 1 通信機器のコンピュータネットワークにおける通信を許可すべくコンピュータネットワークの通信設定を行う設定部とを備える。

【0006】不揮発性メモリは、暗号化された第 1 機器識別情報を格納し、読出部に読み出された第 1 機器識別情報を復号する復号部をさらに備えてもよい。設定部は、第 1 機器識別情報で識別される第 1 通信機器の当該中継機器における通信を許可すべく当該中継機器を設定してもよい。設定部は、第 1 機器識別情報で識別される第 1 通信機器による通信の、当該中継機器における帯域幅をさらに設定してもよい。

【0007】第 1 機器識別情報で識別される第 1 通信機器の当該中継機器に接続された他の中継機器における通信を許可させるように設定させるべく、第 1 機器識別情報を他の中継機器に送信する送信部をさらに備えてもよい。

【0008】他の中継機器は、コンピュータネットワークと、コンピュータネットワークの他のコンピュータネットワークとを接続しており、送信部は、第 1 機器識別情報で識別される第 1 通信機器の他のコンピュータネットワークにおける通信を許可させるように設定させるべく、第 1 機器識別情報を他の中継機器に送信してもよい。

【0009】第 1 機器識別情報で識別される第 1 通信機器のコンピュータネットワークにおける通信を許可するように設定させるべく、コンピュータネットワークを管理する管理装置に、第 1 機器識別情報を送信する送信部をさらに備えてもよい。

【0010】着脱可能な不揮発性メモリを保持する第 2 保持部をさらに有し、読出部は、第 2 保持部に保持された不揮発性メモリから、コンピュータネットワークにおける通信が許可される第 2 通信機器の第 2 機器識別情報を読み出し、設定部は、第 2 機器識別情報で識別される第 2 通信機器のコンピュータネットワークにおける通信を許可すべくコンピュータネットワークの通信設定を行ってもよい。

【0011】設定部は、第 1 機器識別情報で識別される第 1 通信機器の当該中継機器における通信を許可すべく

当該中継機器を設定し、第2機器識別情報で識別される第2通信機器の当該中継機器における通信を許可すべく当該中継機器を設定してもよい。

【0012】第1通信機器が接続される第1接続ポートと、第2通信機器が接続される第2接続ポートとをさらに備え、設定部は、第1通信機器の第1接続ポートにおける通信と、第2通信機器の第2接続ポートにおける通信とを許可すべく、当該中継機器を設定してもよい。設定部は、第1接続ポート及び第2接続ポートを介する通信の帯域幅をさらに設定してもよい。

【0013】当該中継機器における通信を許可する少なくとも1つの通信機器の機器識別情報を格納する記憶部と、記憶部に格納された機器識別情報に基づいて、当該中継機器における通信を許可する通信機器を制限する通信制御部とをさらに備えてもよい。

【0014】設定部は、読出部により読み出された第1機器識別情報で識別される第1通信機器の当該中継機器における通信を許可すべく、読出部により読み出された第1機器識別情報を記憶部に格納してもよい。

【0015】当該中継機器は、複数の通信機器がそれぞれ接続される複数の接続ポートを有し、記憶部は、複数の接続ポートのそれぞれに対応づけて、複数の接続ポートのそれぞれにおける通信を許可する少なくとも1つの通信機器の機器識別情報を格納してもよい。

【0016】本発明の第2の形態によると、コンピュータネットワークの通信設定を行う中継機器用の通信設定プログラムであって、中継機器に、着脱可能な不揮発性メモリから、コンピュータネットワークにおける通信が許可される通信機器の機器識別情報を読み出させる読出モジュールと、機器識別情報で識別される通信機器のコンピュータネットワークにおける通信を許可すべくコンピュータネットワークの通信設定を行わせる設定モジュールとを備える。

【0017】設定モジュールは、機器識別情報で識別される通信機器の当該中継機器における通信を許可させるべく当該中継機器を設定させてもよい。

【0018】機器識別情報で識別される通信機器の当該中継機器に接続された他の中継機器における通信を許可させるように設定させるべく、機器識別情報を他の中継機器に送信させる送信モジュールをさらに備えてもよい。

【0019】本発明の第3の形態によると、コンピュータネットワークにおいて通信を中継する中継機器によるコンピュータネットワークの通信設定方法であって、着脱可能な不揮発性メモリを保持する保持段階と、保持された不揮発性メモリから、コンピュータネットワークにおける通信が許可される通信機器の機器識別情報を読み出す読出段階と、機器識別情報で識別される通信機器のコンピュータネットワークにおける通信を許可すべくコンピュータネットワークの通信設定を行う設定段階とを

備える。

【0020】なお上記の発明の概要は、本発明の必要な特徴の全てを列挙したものではなく、これらの特徴群のサブコンビネーションも又発明となりうる。

【0021】

【発明の実施の形態】以下、発明の実施形態を通じて本発明を説明するが、実施形態はクレームにかかる発明を限定するものではなく、また実施形態の中で説明されている特徴の組み合わせの全てが発明の解決手段に必須であるとは限らない。

【0022】図1は、本発明の一実施形態に係るコンピュータネットワーク100の構成を示す。本実施形態のコンピュータネットワーク100は、コンピュータネットワーク100における通信を中継するスイッチングハブ等の中継機器10a及び10bと、コンピュータネットワーク100における通信を管理する管理装置20と、コンピュータネットワーク100において通信を行う通信機器30a、30b、30c、及び30dとを備える。

【0023】中継機器10a及び10bは、ICカード、ミニチュアカード、フロッピー（登録商標）ディスク等の不揮発性メモリからコンピュータネットワーク100の設定情報を読み出し、コンピュータネットワーク100の通信設定を行う。例えば、中継機器10aは、不揮発性メモリを保持する保持部の一例であるICカードスロットを有し、通信機器30aを使用するユーザによって挿入されたICカードから、通信機器30aの機器識別情報としてMACアドレスを読み出す。そして、中継機器10aは、ICカードから読み出したMACアドレスで識別される通信機器30aの中継機器10aにおける通信を許可すべく、中継機器10aを設定する。

【0024】つまり、通信機器30aを使用するユーザは、通信機器30aを用いてコンピュータネットワーク100に接続するための鍵として、通信機器30aを識別するためのMACアドレスが格納されたICカードを中継機器10aに挿入する。そして、ユーザは、ICカードを中継機器10aに挿入した状態で通信機器30aを使用することにより、コンピュータネットワーク100に進入することができる。また、ICカードを中継機器10aから取り外した場合、ユーザは、通信機器30aによるコンピュータネットワーク100の利用を制限される。例えば、ユーザは、通信機器30aによるコンピュータネットワーク100への進入を禁止されてもよいし、通信機器30b、30c、又は30cに格納されたデータの読み取り等の一定の動作だけが許容されてもよい。

【0025】また、中継機器10aは、ICカードから読み出したMACアドレスで識別される通信機器30aの中継機器10bにおける通信を許可させるべく、ICカードから読み出したMACアドレスを中継機器10b

に送信する。そして、中継機器 10 b は、中継機器 10 a から受信した MAC アドレスで識別される通信機器 30 a の中継機器 10 b における通信を許可すべく、中継機器 10 b を設定する。つまり、通信機器 30 a を使用するユーザは、通信機器 30 a を識別するための MAC アドレスが格納された IC カードを中継機器 10 a に挿入することにより、通信機器 30 a を用いて、中継機器 10 b に接続された通信機器 30 c 及び 30 d と通信することができる。

【0026】また他の例では、中継機器 10 a は、IC カードから読み出した MAC アドレスで識別される通信機器 30 a のコンピュータネットワーク 100 における通信を許可させるべく、IC カードから読み出した MAC アドレスを管理装置 20 に送信する。そして、管理装置 20 は、中継機器 10 a から受信した MAC アドレスで識別される通信機器 30 a のコンピュータネットワーク 100 における通信を許可させるべく、中継機器 10 a 及び 10 b を設定する。そして、通信機器 30 a を使用するユーザは、通信機器 30 a を識別するための MAC アドレスが格納された IC カードを中継機器 10 a に挿入することにより、通信機器 30 a を用いて、コンピュータネットワーク 100 において通信することができる。

【0027】本実施形態に係る中継機器 10 a 及び 10 b によれば、所定のユーザが使用する所定の通信機器がコンピュータネットワーク 100 に進入するための鍵である所定の IC カードを、所定のユーザが所持することによって、所定の IC カードを所持する所定のユーザのみに所定の通信機器によるコンピュータネットワーク 100 への進入を許可することができる。したがって、所定の通信機器と所定の IC カードとの両方を所持する所定のユーザのみにコンピュータネットワーク 100 への進入を許可することができるため、コンピュータネットワーク 100 への不正進入を防ぐことができる。

【0028】また、本実施形態に係るコンピュータネットワーク 100 によれば、中継機器 10 a 及び 10 b において通信機器 30 a、30 b、30 c、及び 30 d によるコンピュータネットワーク 100 への進入を制限するため、中継機器 10 a 及び 10 b において通信が許可されない通信機器は、管理装置 20 への接続を許可されないこともできる。そのため、本実施形態に係るコンピュータネットワーク 100 によれば、不正進入に対するセキュリティが非常に高いコンピュータネットワークシステムを実現することができる。

【0029】図 2 は、本実施形態に係る中継機器 10 a の構成を示す。中継機器 10 a と中継機器 10 b とは、同一の構成を有しており、以下において、代表して中継機器 10 a の構成及び動作について説明する。

【0030】中継機器 10 a は、着脱可能な不揮発性メモリを保持する保持部 102 a、102 b、102 c、

102 d、102 e、及び 102 f と、不揮発性メモリから通信機器の機器識別情報を読み出す読出部 104 と、暗号化された機器識別情報を復号する復号部 106 と、読み出された機器識別情報で識別される通信機器のコンピュータネットワーク 100 における通信を許可すべくコンピュータネットワーク 100 の通信設定を行う設定部 108 と、中継機器 10 a における通信が許可された少なくとも 1 つの通信機器の機器識別情報を格納する記憶部 110 と、機器識別情報を受受信する送受信部 112 と、中継機器 10 a における通信を許可する通信機器を制限する通信制御部 114 と、通信機器が接続される接続ポート 116 a、116 b、116 c、116 d、116 e、及び 116 f とを備える。

【0031】保持部 102 a、102 b、102 c、102 d、102 e、及び 102 f は、通信機器の機器識別情報が格納された不揮発性メモリを保持する。そして、読出部 104 は、保持部 102 a、102 b、102 c、102 d、102 e、又は 102 f に保持された不揮発性メモリから、コンピュータネットワーク 100 における通信が許可される通信機器の機器識別情報を読み出す。復号部 106 は、不揮発性メモリから読み出された機器識別情報が暗号化されている場合、暗号化された機器識別情報を復号する。そして、復号部 106 は、復号した機器識別情報を設定部 108 に供給する。

【0032】次に、設定部 108 は、不揮発性メモリから読み出された機器識別情報で識別される通信機器のコンピュータネットワーク 100 における通信を許可すべくコンピュータネットワーク 100 の通信設定を行う。まず、設定部 108 は、不揮発性メモリから読み出された機器識別情報で識別される通信機器の中継機器 10 a における通信を許可すべく、中継機器 10 a を設定する。具体的には、設定部 108 は、不揮発性メモリから読み出された機器識別情報を記憶部 110 に格納することにより、不揮発性メモリから読み出された機器識別情報で識別される通信機器の中継機器 10 a における通信を可能にする。

【0033】次に、通信制御部 114 は、記憶部 110 に格納された機器識別情報に基づいて、中継機器 10 a における通信を許可する通信機器を制限する。つまり、通信制御部 114 は、不揮発性メモリから読み出され、記憶部 110 に格納された機器識別情報で識別される通信機器の中継機器 10 a における通信を許可する。例えば、通信制御部 114 は、送受信部 112 によって受信されたデータのヘッダ情報を参照し、ヘッダ情報に含まれる送信元の通信機器の機器識別情報が記憶部 110 に格納されている場合、送受信部 112 に対して当該データの送信を許可する。

【0034】また、送受信部 112 は、中継機器 10 a における通信を許可する通信機器の機器識別情報を中継機器 10 b から受信する。そして、設定部 108 は、送

受信部 112 が受信した機器識別情報を記憶部 110 に格納することにより、送受信部 112 が受信した機器識別情報で識別される通信機器の中継機器 10a における通信を可能にする。

【0035】また、送受信部 112 は、不揮発性メモリから読み出された機器識別情報で識別される通信機器の、中継機器 10a に接続された中継機器 10b における通信を許可させるべく、不揮発性メモリから読み出された機器識別情報を中継機器 10b に送信してもよい。また、送受信部 112 は、不揮発性メモリから読み出された機器識別情報で識別される通信機器の、コンピュータネットワーク 100 における通信を許可するように設定させるべく、コンピュータネットワーク 100 を管理する管理装置 20 に、不揮発性メモリから読み出された機器識別情報を送信してもよい。

【0036】また、設定部 108 は、不揮発性メモリから読み出された機器識別情報で識別される通信機器による通信の、中継機器 10a における帯域幅を設定してもよい。例えば、設定部 108 は、複数の接続ポートのそれぞれに対して、優先順位を設定してもよい。また、設定部 108 は、複数の接続ポートのそれぞれに対して、帯域幅の上限を設定してもよい。

【0037】また、保持部 102a、102b、102c、102d、102e、及び 102f のそれぞれと、接続ポート 116a、116b、116c、116d、116e、及び 116f のそれぞれとは、対応づけられてもよい。つまり、通信制御部 114 は、保持部 102a に保持された不揮発性メモリから読み出された機器識別情報に基づいて、接続ポート 116a に接続された通信機器の中継機器 10a における通信を制限し、保持部 102b に保持された不揮発性メモリから読み出された機器識別情報に基づいて、接続ポート 116b に接続された通信機器の中継機器 10a における通信を制限してもよい。

【0038】例えば、読出部 104 は、保持部 102a に保持された不揮発性メモリから、コンピュータネットワーク 100 における通信が許可される通信機器 30a の機器識別情報を読み出す。また、読出部 104 は、保持部 102b に保持された不揮発性メモリから、コンピュータネットワーク 100 における通信が許可される通信機器 30b の機器識別情報を読み出す。

【0039】次に、設定部 108 は、保持部 102a に保持された不揮発性メモリから読み出された機器識別情報で識別される通信機器 30a による接続ポート 116a における通信を許可すべく、記憶部 110 に機器識別情報を格納する。また、設定部 108 は、保持部 102b に保持された不揮発性メモリから読み出された機器識別情報で識別される通信機器 30b による接続ポート 116b における通信を許可すべく、記憶部 110 に機器識別情報を格納する。そして、通信制御部 114 は、記

憶部 110 に格納された機器識別情報に基づいて、通信を許可する通信機器を制限する。

【0040】また、通信制御部 114 は、中継機器 10b の保持部に保持された不揮発性メモリから読み出された機器識別情報に基づいて、中継機器 10b に接続された通信機器 30c 及び 30d の中継機器 10a における通信を制限してもよい。また、設定部 108 は、接続ポート 116a、116b、116c、116d、116e、及び 116f を介する通信の帯域幅を設定してもよい。

【0041】本実施形態に係る中継機器 10a によれば、不揮発性メモリから、暗号化された通信機器の機器識別情報を読み出して復号するため、不揮発性メモリに格納された機器識別情報の漏洩を防ぐことができる。また、本実施形態に係る中継機器 10a によれば、中継機器 10a に挿入された不揮発性メモリに格納された設定情報に基づいて、通信機器毎又は接続ポート毎の中継機器 10a における帯域幅を設定できるため、コンピュータネットワーク 100 における通信路を効率的に利用することができる。また、本実施形態に係るコンピュータネットワーク 100 によれば、中継機器毎にそれぞれの中継機器における通信が許可された通信機器を制限するため、不正進入に対するセキュリティが非常に高いコンピュータネットワークシステムを実現することができる。

【0042】図 3 は、記憶部 110 に格納される通信制御ファイルのデータフォーマットの一例を示す。通信制御ファイルは、接続ポート番号フィールド及び機器識別情報フィールドを有する。接続ポート番号フィールドは、通信機器が有する複数の接続ポートを識別するために割り当てられた接続ポート番号を格納する。機器識別情報フィールドは、通信機器を識別するための識別情報を格納する。例えば、機器識別情報フィールドは、MAC アドレスを格納する。

【0043】なお、本実施形態において、接続ポート 116a の接続ポート番号は 1、接続ポート 116b の接続ポート番号は 2、接続ポート 116c の接続ポート番号は 3、接続ポート 116d の接続ポート番号は 4、接続ポート 116e の接続ポート番号は 5、接続ポート 116f の接続ポート番号は 6 とする。

【0044】通信制御ファイルは、複数の接続ポートのそれぞれに対応づけて、複数の接続ポートのそれぞれにおける通信を許可する少なくとも 1 つの通信機器の機器識別情報を格納する。例えば、通信制御部 114 は、所定の接続ポートから受信したデータのヘッダ情報を参照し、ヘッダ情報に含まれる送信元の通信機器の機器識別情報が、前記所定の接続ポートに対応づけて格納されている場合、送受信部 112 に対して当該データの送信を許可する。

【0045】また、通信機器を識別する機器識別情報を

格納する不揮発性メモリが、通信機器を使用するユーザによって、保持部102a、102b、102c、102d、102e、又は102fに挿入されることにより、不揮発性メモリに格納された機器識別情報が通信制御ファイルに格納される。また、ユーザによって、保持部102a、102b、102c、102d、102e、又は102fから不揮発性メモリが取り外されることによって、不揮発性メモリに格納された機器識別情報が通信制御ファイルから削除される。

【0046】通信制御部114は、機器識別情報1A251F33262Dで識別される通信機器の、接続ポート番号が1である接続ポート116aにおける通信を許可する。また、通信制御部114は、機器識別情報3F3610152A1Bで識別される通信機器の、接続ポート番号が2である接続ポート116bにおける通信を許可する。また、通信制御部114は、機器識別情報2B1A392A181Cで識別される通信機器の、接続ポート番号が4である接続ポート116dにおける通信を許可する。

【0047】また、通信制御部114は、機器識別情報1C2A361F253Bで識別される通信機器、及び機器識別情報2B2D2A15361Fで識別される通信機器の、接続ポート番号が6である接続ポート116fにおける通信が許可される。これは、接続ポート116fに接続された中継機器10bの接続ポートに機器識別情報1C2A361F253Bで識別される通信機器、及び機器識別情報2B2D2A15361Fで識別される通信機器が接続されている場合である。

【0048】本実施形態に係る中継機器10aによれば、複数の接続ポートのそれぞれに対して、複数の接続ポートのそれぞれにおける通信を許可する通信機器を制限することにより、所定の接続ポートにおいては所定の通信機器による通信のみを許可することができるため、不正進入に対するセキュリティが非常に高いコンピュータネットワークシステムを実現することができる。

【0049】図4は、コンピュータネットワーク100とコンピュータネットワーク200との構成の一例を示す。コンピュータネットワーク100は、図1に示した構成と同様である。コンピュータネットワーク200は、コンピュータネットワーク200における通信を中継するスイッチングハブ等の中継機器10cと、コンピュータネットワーク200において通信を行う通信機器30e及び30fとを備える。コンピュータネットワーク100とコンピュータネットワーク200とは、セグメントが異なり、ブリッジ、ルータ等の中継機器40を介して接続される。

【0050】通信機器30aを使用するユーザが、中継機器10aの保持部102aに不揮発性メモリを挿入する。そして、中継機器10aは、通信機器30aのコンピュータネットワーク200における通信を許可させる

べく、不揮発性メモリから読み出した通信機器30aを識別する機器識別情報を、中継機器10bを介して中継機器40に送信する。そして、中継機器40は、中継機器10aから受信した機器識別情報で識別される通信機器30aの中継機器40における通信を許可する。そして、通信機器30aは、セグメントが異なるコンピュータネットワーク200が有する通信機器30e及び30fと通信することができる。

【0051】本実施形態に係る中継機器10aによれば、通信機器のユーザは、当該通信機器に直接接続される中継機器に不揮発性メモリを挿入することにより、当該通信機器が属するセグメントと異なるセグメントのコンピュータネットワークへの進入を可能にすることができる。

【0052】図5は、管理装置20のハードウェア構成を示す。管理装置20は、CPU700と、ROM702と、RAM704と、通信インタフェース706と、ハードディスクドライブ708と、データベースインタフェース710と、フロッピーディスクドライブ712と、CD-ROMドライブ714とを備える。CPU700は、ROM702及びRAM704に格納されたプログラムに基づいて動作し、各部の制御を行う。通信インタフェース706は、コンピュータネットワークを介して中継機器10aと通信する。データベースインタフェース710は、データベースへのデータの書込、及びデータベースの内容の更新を行う。

【0053】フロッピーディスクドライブ712は、フロッピーディスク720からデータ又はプログラムを読み取り通信インタフェース706に提供する。CD-ROMドライブ714は、CD-ROM722からデータ又はプログラムを読み取り通信インタフェース706に提供する。通信インタフェース706は、フロッピーディスクドライブ712又はCD-ROMドライブ714から提供されたデータ又はプログラムを中継機器10aに送信する。データベースインタフェース710は、各種データベース724と接続してデータを送受信する。

【0054】中継機器10aに提供されるプログラムは、フロッピーディスク720又はCD-ROM722等の記録媒体に格納されて利用者によって提供される。記録媒体に格納されたプログラムは圧縮されていても非圧縮であってもよい。プログラムは記録媒体から読み出され、通信インタフェース706を介して、中継機器10aにインストールされ、中継機器10aにおいて実行される。

【0055】記録媒体に格納されて提供されるプログラム、即ち中継機器10aにインストールされるプログラムは、機能構成として、読出モジュールと、設定モジュールと、復号モジュールと、送信モジュールと、記憶モジュールと、通信制御モジュールとを有する。各モジュールが中継機器10aに働きかけて行わせる動作は、図

1 から図 4 において説明した中継機器 10 a における、対応する部材の動作と同一であるから、説明を省略する。

【0056】図 5 に示した、記録媒体の一例としてのフロッピーディスク 720 又は CD-ROM 722 には、本出願で説明した全ての実施形態における中継機器 10 a の動作の一部又は全ての機能を格納することができる。

【0057】これらのプログラムは記録媒体から直接中継機器 10 a によって読み出されて実行されても、中継機器 10 a にインストールされた後に中継機器 10 a において実行されてもよい。更に、上記プログラムは単一の記録媒体に格納されても複数の記録媒体に格納されてもよい。又、符号化した形態で格納されていてもよい。

【0058】記録媒体としては、フロッピーディスク、CD-ROM の他にも、DVD、PD 等の光学記録媒体、MD 等の光磁気記録媒体、テープ媒体、磁気記録媒体、IC カードやミニチュアカードなどの半導体メモリ等を用いることができる。また、専用通信ネットワークやインターネットに接続されたサーバシステムに設けたハードディスク又は RAM 等の格納装置を記録媒体として使用し、通信網を介してプログラムを中継機器 10 a に提供してもよい。このような記録媒体は、中継機器 10 a を製造するためのみに使用されるものであり、そのような記録媒体の業としての製造及び販売等が本出願に基づく特許権の侵害を構成することは明らかである。

【0059】以上、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記実施形態に記載の範囲には限定されない。上記実施形態に、多様な変更又は改良を加えることができる。そのような変更又は改良を加えた形態も本発明の技術的範囲に含まれ得ることが、特許請求の範囲の記載から明らかである。

【0060】

【発明の効果】上記説明から明らかなように、本発明によれば、不正進入に対するセキュリティが非常に高いコンピュータネットワークシステムを実現できる中継機器

を提供することができる。

【図面の簡単な説明】

【図 1】コンピュータネットワーク 100 の構成図である。

【図 2】中継機器 10 a の構成図である。

【図 3】記憶部 110 に格納される通信制御ファイルのデータフォーマットである。

【図 4】コンピュータネットワーク 100 とコンピュータネットワーク 200 との構成図である。

【図 5】管理装置 20 のハードウェア構成図である。

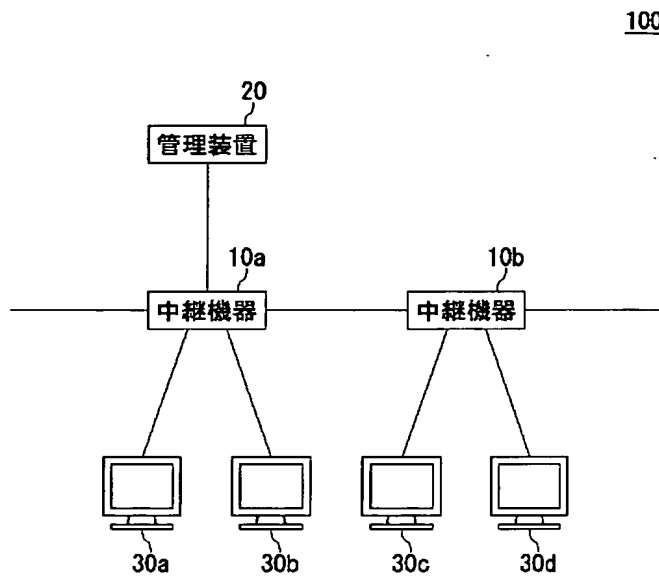
【符号の説明】

10 a ~ 10 c 中継機器
20 管理装置
30 a ~ 30 f 通信機器
40 中継機器
100 コンピュータネットワーク
102 a ~ 102 f 保持部
104 読出部
106 復号部
108 設定部
110 記憶部
112 送受信部
114 通信制御部
116 a ~ 116 f 接続ポート
200 コンピュータネットワーク
700 CPU
702 ROM
704 RAM
706 通信インタフェース
708 ハードディスクドライブ
710 データベースインタフェース
712 フロッピーディスクドライブ
714 CD-ROM ドライブ
720 フロッピーディスク
722 CD-ROM
724 各種データベース

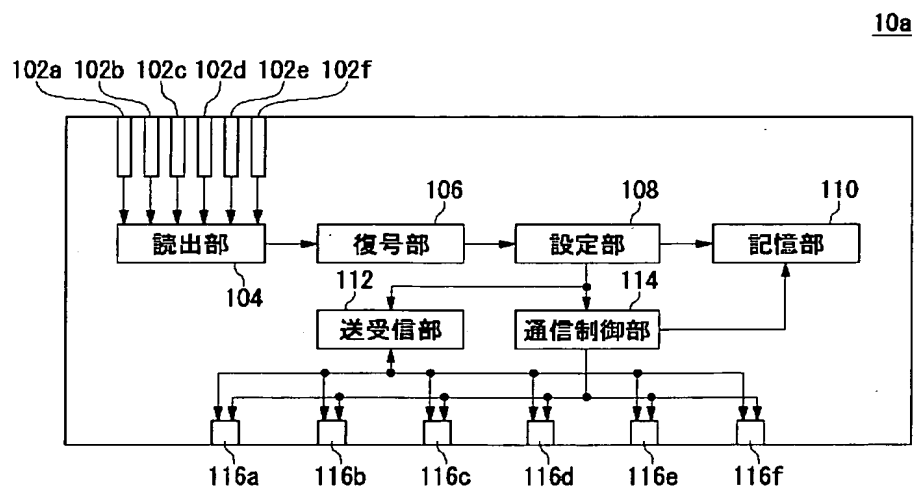
【図 3】

接続ポート番号	機器識別情報
1	1A251F33262D
2	3F3610152A1B
3	
4	2B1A392A181C
5	
6	1C2A361F253B, 2B2D2A15361F

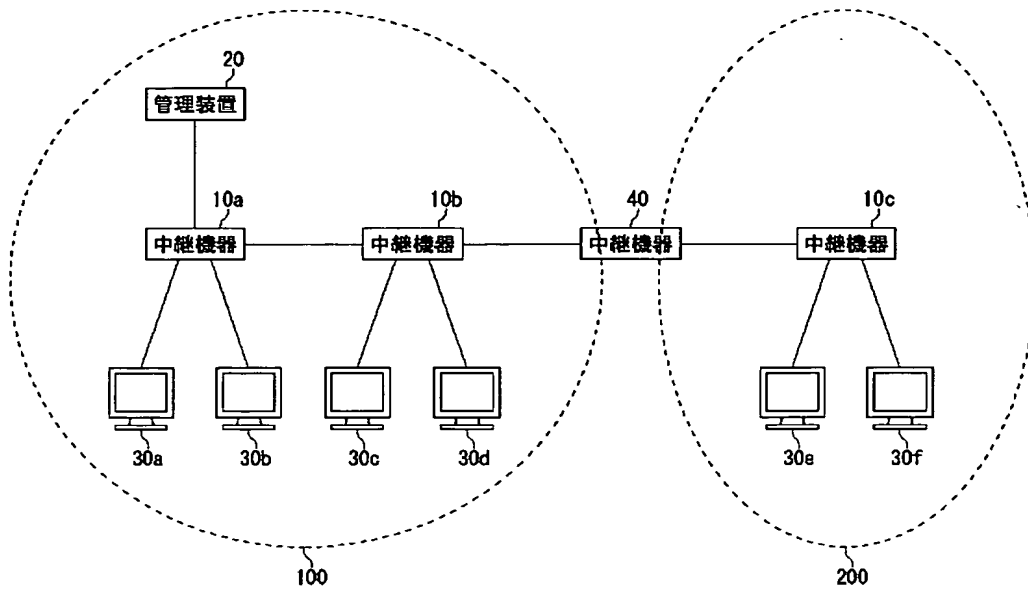
【図 1】



【図 2】



【図 4】



【図 5】

